

Internet Safety Quick Reference Guide

1 Before you login

Don't save your logon information

- If the option is presented to you, always say no; never save passwords!

Don't leave the computer unattended with sensitive information on the screen

- When leaving the public computer, log out of all programs and close all windows that might display sensitive information.

2 After you login

Whether checking your email, bank account, or health record, it is important to be safe. Protect your sensitive information.

Watch for over-the-shoulder snoops

- When using a public computer, be on the lookout for thieves who look over your shoulder or watch as you enter sensitive passwords to collect your information.

Don't save personal documents on the library computer.

- Use a USB drive to save or download a document. Anything saved on the library computer can be viewed by everyone who uses the library computer.
- If you save and then delete something on the library computer, empty the Recycle Bin so the hard drive does not have a trace.
- Don't send personal information by email.

If you print something, pick it up immediately.

3 Before you leave

Even if it is just to pick up a printout or make a quick trip to the bathroom.

Erase your tracks

- Disable the tracking features of your browser (more information on back of this page).
- After using a public computer, protect your private information by deleting the temporary Internet files (more information on back of this page).
- People sometimes leave their belongings like computer printouts, USB drives, bags, cell phones, pens, books, or even some important information scribbled on paper. Always be careful with your personal belongings in public places.

Additional information:

1 Before you login

Create secure passwords. Do not use something obvious such as a birthday, a mother's name, a pet name, a social security number, etc.

- Add numbers and other symbols (*&^%\$#@) to the password.
- Make the password at least 10 characters in length.
- Use upper case and lower case letters within the password.
- Do not write the password down anywhere.
- Do not reuse passwords.

2 After you login

Do not download any file where you do not recognize the source. It could contain malicious material.

When on the Internet, limit the amount of information shared over the Internet.

- Avoid sharing phone numbers, addresses, birth date, and social security number.
- If you must share this information, a firewall, antivirus, a secure network with encryption, and a strong password for the account will help keep the information more secure.

A secure website is identified by the "https" at the beginning of a web address. The "s" stands for secure, meaning the information entered on that site will be encrypted.

- A padlock icon next to the web address means that it is secure.
- "Spoof" websites with the "https" or the padlock icon can be created. Check the website's security by double-clicking on the padlock. An "issued to" window will pop-up with the name of the website; if it does not match the website name that you should be on, then it could be a duplicated spoof site.

When opening an email, be aware of whom the email is from. If you do not know the person or company, delete it.

Don't open email attachments unless you know the sender. Attachments are a common way for people to send out viruses, worms, Trojans, etc.

3 Before you leave

Fully log off all accounts accessed during your session on the computer. Do not just "x" out of a window. Use the "log off" button that is provided.

- After logging off of all accounts, delete the browser history so the next user can't see what websites were visited.
 - This can be done using the toolbar on the top of the webpage. Click on the heading "safety" or "tools". Look for the option to delete browsing history.
 - Find more information at www.hotcomm.com/faq/faq_temp_files.asp or www.computerhope.com/issues/ch000510.htm.